IN THE UNITED STATES DISTRICT COURT

FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

In the Matter of the Search of:		
A 2TB Hitachi Hard Drive Serial Number YFGNBBTA and Labeled HD-2	:	Case No. 1:18mj307

DEFENDANT'S RESPONSE TO GOVERNMENT'S APPLICATION FOR AN ORDER TO REQUIRE DEFENDANT BURNS TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT PURSUANT TO THE ALL WRITS ACT

NOW COMES the Defendant, by and through the undersigned counsel, and hereby requests that the Court deny the government's Application for an order compelling Timothy Donovan Burns to produce the 2TB Hitachi hard drive, currently in the custody of Homeland Security Investigations (HSI), in an unlocked and decrypted state. The All Writs Act is not applicable to this case, as the government has not shown such relief is necessary and appropriate. The Self-Incrimination Clause of the Fifth Amendment of the United States Constitution states that "no person…shall be compelled in any criminal case to be a witness against himself" and the government is attempting to circumvent the Fifth Amendment by seeking a writ to force Mr. Burns to decrypt seized devices. U.S. Const. amend V.

I. ALL WRITS ACT INAPPLICABLE AS GOVERNMENT HAS FAILED TO PROVE SUCH RELIEF IS NECESSARY AND APPROPRIATE

The All Writs Act requires the writ be "necessary and appropriate" before the court can order relief. 28 U.S.C. §1651(a). The government has only given vague details about attempts to decrypt and have made no attempt for third party intervention from the software manufacturer. In applying for an Order under the All Writs Act to force Mr. Burns to decrypt his devices, the government implies they have no other means to obtain the evidence and their last resort is to ignore the Fifth Amendment.

Federal courts may issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principle of law." 28 U.S.C. §1651(a). The government has failed to show such an order either necessary or appropriate. The description of the HSI attempt to gain access to the devices is vague at best and does not demonstrate a need so pressing as to be either necessary or appropriate, let alone sufficient to extinguish Mr. Burns' Constitutional rights. Once the evidence is made available, there is no adequate remedy for Mr. Burns to regain his rights and protections under the Fifth Amendment.

For the 2TB Hitachi Hard Drive, HSI has attempted to break the encryption through brute-force decryption. Brute-force

decryption is simply an automated trial and error process to produce the correct password through "exhaustive effort rather than employing intellectual strategies." *Brute Force Attack*. TechTarget. https://searchsecurity.techtarget.com/definition/brute-force-cracking (accessed March 14, 2019). According to the Government's Application, these efforts have been unsuccessful. *Gov't Application Under the All Writs Act*, p. 8.

Several cases the government cited for the All Writs Act jurisdiction involve third party manufacturers. The seminal case, *U.S. v. New York Tel. Co.*, involved the government requesting a writ to require a neutral third party to install pen registers to effectuate a warrant against a defendant. *U.S. v. New York Tel. Co.*, 434 U.S. 159, 98 S.Ct. 364, 54 L.Ed.2d 376 (1977). In *Blake*, the court ordered Apple Inc. to assist the FBI by bypassing an iPad's security measures. *United States v. Blake*, 868 F.3d 960, 971 (11th Cir. 2017).

By going to the third party manufacturers, the government could avoid direct Fifth Amendment implications and possibly obtain the assistance they need without forcing Mr. Burns to be a witness against himself.

The United States District Court of Maryland noted that *N.Y. Telephone Company* and its application to the All Writs Act does not grant a court "unbridled power." *In re Application of*

U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 579 (D. Md. 2011)(" *N.Y. Telephone Company* does not grant the Court an unbridled inherent power to infringe on an individual's privacy rights, outside of the governing structure of the Fourth Amendment."). The All Writs Acts enables courts to issue supplemental orders to effectuate valid issued orders or warrants but can only do so "in the absence of other enabling authority" and "only to the extent any supplemental order issued does not constitute an additional invasion of privacy." *Id.* The Maryland District Court noted an important distinction regarding *N.Y. Telephone Company*—the Supreme Court acknowledged and deferred to congressional approval of a pen register as a permissible law enforcement tool. *Id.* Congress has not approved of directly using defendants as a permissible law enforcement tool in their own case. These laws would fly right in the face of long standing Constitutional protections.

The *In re Application* Court, following the direction of multiple Supreme Court and Circuit Court decisions, determined that the intent of the All Writs Act is to provide courts with the "instruments needed to perform their duty, as prescribed by the Congress and the Constitution," *Id* at 580 (citing *Harris v. Nelson,* 394 U.S. 286, 300, 89 S.Ct. 1082, 22 L.Ed.2d 281 (1969)) (citing *Price v. Johnston,* 334 U.S. 266, 282, 68 S.Ct.

1049, 92 L.Ed. 1356 (1948)), so as "to process litigation to a just and equitable conclusion." *ITT Comm. Dev. Corp. v. Barton*, 569 F.2d 1351, 1359 (5th Cir.1978). To this end, the All Writs Act is a "gap-filling measure," and just because a "party may be assisted in its discharge of it rights or duties by the issuance of a writ is not sufficient basis for the writ." *Id* (citing *Barton*, 569 F.2d at 1360).

The government has only shown minimal attempts at decryption and has only mentioned rudimentary methods that would not implicate the Fifth Amendment by requiring Mr. Burns's assistance. There is no evidence the government has contacted VeraCrypt (makers of the software at issue) or any other manufacturer for assistance with the decryption. Application of the All Writs Act to a third party not at issue in the case is well settled law. Furthermore, there is no evidence that the government has attempted to exploit weaknesses in the VeraCrypt Software in an effort to decrypt.

The government has failed to prove the very basis of jurisdiction for relief under the All Writs Act: that such relief is necessary and appropriate. Therefore, the government is not entitled to relief under the Act and the Application should be denied.

II. FORCING MR. BURNS TO DECRYPT HIS DEVICES IS A VIOLATION OF HIS FIFTH AMENDMENT RIGHT AGAINST SELF-INCRIMINATION

The information the government seeks, and the manner in which they seek it, adheres directly to the qualifications for Fifth Amendment privileges. To qualify for the Fifth Amendment privilege, an act or communication must be (1) testimonial, (2) incriminating, and (3) compelled. *Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County, et al.*, 542 U.S. 177, 189, 124 S.Ct. 2451, 159 L.Ed.2d 292 (2004). Forced decryption provides, at a minimum, a potential link in a chain of incriminating evidence. *Hoffman v. United States*, 341 U.S. 479, 486, 71 S.Ct. 814, 95 L.Ed 1118 (1951) (holding that the Fifth Amendment covers evidence "which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime"). Although the passwords themselves are not incriminating, Mr. Burns' actions are still protected by the Fifth Amendment. U.S. Const. amend. V.

The government instead is choosing to rely on the "foregone conclusion" doctrine and whether forcing him to decrypt devices would be "compelling" him to provide testimony. Granting this order would be an irreparable and irreversible violation of Mr. Burns's rights. The government appears to concede the incriminating and testimonial prongs to qualify Mr. Burns to

claim a Fifth Amendment privilege against the compelled production of his seized devices in an unencrypted state.

A. FORCING MR. BURNS TO DECRYPT DEVICES WOULD BE COMPELLED TESTIMONY IN VIOLATION OF THE FIFTH AMENDMENT

"It has, however, long been settled that [the Fifth Amendment's] protection encompasses compelled statements that lead to the discovery of incriminating evidence even though the statements themselves are not incriminating. Compelled testimony that communicates information that may 'lead to incriminating evidence' is privilege even if the information itself is not inculpatory." *United States v. Hubbell*, 530 U.S. 27, 37-38, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000). The government is not seeking passwords themselves but rather the devices and software in an unencrypted state. Such an action is compelled, as it forces Mr. Burns to express the contents of his mind. *See Doe v. United States*, 487 U.S. 201, 219, 108 S. Ct. 2341, 2352, 101 L. Ed. 2d 184 (1988) (Stevens, J., dissenting). Most cases simply conceded the issue and the discussion surrounds whether the action is testimonial or a foregone conclusion. Forcing someone to provide evidence against themselves, even if they voluntarily created the evidence, is compelling testimony because it establishes a necessary element of the offenses: possession and control.

"The elements of compulsion are clearly present, but the more difficult issues are whether the tacit averments of the

taxpayer are both "testimonial" and "incriminating" for purposes of applying the Fifth Amendment." *Fisher v. U.S.*, 425 U.S. 391, 410-11, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976). In *Fisher*, the attorneys for two different taxpayers were sent subpoenas to produce working documents created by the taxpayer's accountants. The taxpayer's were not subpoenaed and they were not required to give oral testimony about the contents of the documents. Unlike Mr. Burns's case, the mere possession of the documents was not a crime.

> Moreover, assuming that these aspects of producing the accountant's papers have some minimal testimonial significance, surely it is not illegal to seek accounting help in connection with one's tax returns or for the accountant to prepare workpapers and deliver them to the taxpayer. At this juncture, we are quite unprepared to hold that either the fact of existence of the papers or of their possession by the taxpayer poses any realistic threat of incrimination to the taxpayer.

Fisher v. U.S., 425 U.S. 391, 412 (1976)

Despite the government's assertion to the contrary, the element of compulsion is clearly present because the government is demanding Mr. Burns produce the contents of his mind and admit possession (an element of the charged offense) by forcing him to decrypt devices in the government's possession. Mr. Burns has not been offered immunity from prosecution so he cannot be compelled to decrypt the target devices.

> Given out conclusion that respondent's act of production has a testimonial aspect, at least with

> respect to the existence and location of the documents sought by the Government's subpoena, respondent could not be compelled to produce those documents without first receiving a grant of immunity under § 6003.

U.S. v. Hubbell, 530 U.S. 27, 45 (2000)

In *Hubbell*, the Court confirmed that an act is testimonial if it *implicitly or tacitly* communicates a statement of fact, including an admission that something was in the suspect's "possession or control." 530 U.S. at 36; *see also Doe v. United States*, 487 U.S. 201, 209, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988) ("*Doe II*"); *Fisher*, 425 U.S. at 410. An act can be testimonial even if the disclosure itself is not incriminating evidence (there is incriminating evidence on the device). *See Hubbell*, 530 U.S. at 37-38. In *Hubbell*, the defendant was granted immunity from prosecution under 18 U.S.C. §6003(a), which compelled him to cooperate in the investigation due to his immunity. It is that grant of immunity that overcame his Fifth Amendment objections and resulted in the compelled production of documents. Unlike the defendant in *Hubbell*, *Fricosu*, and *Blake*, Mr. Burns has not been offered immunity in any form at this time.

The Supreme Court has made clear that the Fifth Amendment privilege applies to not just words, but also *acts*, that imply assertions of fact. *Doe v. United States*, 487 U.S. 201, 209 (1988) ("Doe II"). The Court has defined the test for a

"testimonial" act in that it "must itself, explicitly or implicitly, relate a factual assertion or disclose information." *United States v. Hubbell*, 530 U.S. 27, 36, n.9 (2000); *Hiibel*, 542 U.S. at 189. An act of production may have "communicative aspects of its own, wholly aside from the contents of the papers produced." *United States v. Fisher*, 425 U.S. 391, 410 (1976).

The most recent jurisdiction to apply our current jurisprudence to the ever-changing landscape of technological issues is the Northern District of California. In its decision from January 10, 2019, the Court concluded that forcing a defendant to unlock an electronic device through biometrics (i.e. Face I.D. or Touch I.D.) infringed on a defendant's Fifth Amendment rights. *Matter of Residence in Oakland, California*, 354 F. Supp. 3d 1010 (N.D. Cal. 2019). While possibly expediting a search, compelling a defendant to unlock an electronic device in this manner was an "abuse of power" and "unconstitutional." *Id*.

In fashioning its decision that *Matter of Residence* court distinguished the compelled access of an electronic device through biometrics from submitting to a fingerprinting or DNA swab. In doing so, the Court relied on *Doe II* and *Schmerber* in finding that these two actions are not the same. *Id* (citing *Schmerber v. California*, 384 U.S. 757, 764, 86 S.Ct. 1826, 16 L.Ed.2d 908 (1966) ("The distinction which has emerged, often

expressed in different ways, is that the privilege is a bar against compelling 'communications' or 'testimony,' but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it.")); see also *Doe v. United States*, 487 U.S. at 210, 108 S.Ct. 2341.

Forcing Mr. Burns to produce his devices in an unencrypted state would compel him to provide testimony against himself in violation of the Fifth Amendment of the United States Constitution. U.S. Const. amend. V.

B. INCRIMINATING

The government concedes this element as they argue under "foregone conclusion" the contents of the decrypted devices would be likely incriminating. *Gov't Application Under the All Writs Act*, p. 17. The government then attempts to backtrack from this concession by saying that knowledge of the encryption password does not necessarily imply knowledge of the device's contents. *Id.* This concept directly contradicts a necessary element for the government to succeed under *Apple Macpro*—that the "files exist[ed] on the encrypted portions" of the hard drive and that the defendant "[could] access them." 851 F.3d at 248.

C. TESTIMONIAL

The government concedes the requested decryption would be testimonial.

> Accordingly, the government proceeds on the assumption that the production here of the unencrypted electronic devices includes the potentially testimonial aspects of the act of production in Fisher-namely, that the targeted hard drive exists and belongs to Burns, that the Burns can decrypt the hard drive, and that the hard drive contains child pornography.

Gov't Application Under the All Writs Act, p. 18.

A compelled act is "testimonial": when the act reveals an implicit or tacit admission that something is in the person's "possession or control." *See Hubbell*, 530 U.S. at 36; *Doe II*, 487 U.S. at 209. In *Hubbell*, the Supreme Court held that the defendant's act of producing documents compelled by a subpoena was "testimonial" because the act implicitly communicated, among other pieces of information, that the defendant possessed incriminating documents. 530 U.S. at 43-45. Like the facts in *Hubbell*, in this case, a person's compelled access to a hard drive by forcing them to decrypt the hard drive would be testimonial. This is consistent with *Matter of Residence*, deciding that compelled access to a device through biometric Touch I.D. or Face I.D. would be testimonial because it would implicitly communicate that the person possessed or controlled that device with incriminating evidence on it. 354 F. Supp. 3d 1010 (N.D. Cal. 2019)

The ability to access a device through biometrics or inputting a password also discloses that the person could decrypt, retrieve, and examine its data and contraband whenever

he or she wishes, which is particularly inculpatory in a child pornography investigation.

This point is amplified by a comparison to the facts of the Supreme Court's ruling in *Doe II*, 487 U.S. 201. In *Doe II*, the Court found that compelling a defendant to sign a generic consent form authorizing the release of bank records—but without any reference to particular bank accounts—would not be "testimonial." 487 U.S. at 215-16. The Court reasoned this was because the defendant, in signing the form, would not be acknowledging control of any *particular* bank account. *Id.* at 215. In contrast here, the compelled access would reveal exactly what particular device the person possessed or controlled—the one they had just accessed through biometrics or password. If Mr. Burns succeeds in unlocking the 2TB Hitachi Hard Drive, there is no divorcing the compelled act of production from the resulting implicit testimony that he possesses and controls the device and any contraband or evidence stored on it.

Forced access through inputting a password would also be "testimonial" in a second, alternative way: decryption of the contents of the devices will occur if they are unlocked by forced access. Decryption if defined as "to decode or decipher." *Dictionary.com Unabridged*. Random House, Inc. http://www.dictionary.com/browse/decryption (accessed: March 14, 2019).

In other words, the single forced act by Mr. Burns would (1) unlock the devices (and related data) and (2) decrypt the information contained on the device. This decryption would be "testimonial" because it would translate otherwise unintelligible data into a form that can be used and understood by investigators. Encryption does significantly more than lock up data; it transforms it into a scrambled, unintelligible format.[1] When information on a phone, computer, or other electronic device is encrypted, it exists only in its scrambled format. Thus, breaking into an encrypted device would allow access to only indecipherable data. The information needs to be decrypted—translated into a form that can be used and understood—in order to be of any value to law enforcement. It is this translation that is the "testimonial" component for the Fifth Amendment analysis.

Forced decryption encroaches on "the right of each individual 'to a private enclave where he may lead a private life.'" *See Doe II*, 487 U.S. at 212. "Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records, and

[1] Encryption technology allows a person to transform plain, *U.S. v. Apple MacPro Computer*, 851 F.3d 238, 242 (3d Cir. 2017)

private emails." *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013). As the Supreme Court recently acknowledged in *Riley v. California*, 134 S.Ct. 2473, 2490, 189 L.Ed.2d 430 (2014), mobile phones and electronic devices contain "a digital record of nearly every aspect of [users'] lives—from the mundane to the intimate." Thus, electronic devices, "[w]ith all they contain and all they reveal, they hold for many Americans 'the privacies of life.'" *Id.* at 2494-95 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

In the case of *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011,* 670 F. 3d 1335, 1349 (11th Cir. 2012), the Eleventh Circuit confronted the scope of Fifth Amendment protection in the context of compelled decryption in a child pornography case, and concluded that the suspect's refusal to decrypt various digital media seized pursuant to a search warrant was conduct protected under the right against self-incrimination. In reaching this conclusion, the Court of Appeals reversed the District Court and found that it erred when it held that the requested decryption and production of hard drives was not testimonial. *Id.* at 1341.

Forced decryption is inherently compelled and testimonial. The likely incriminating nature of the information has already been established. The Fifth Amendment's self-incrimination privilege "enables the citizen to create a zone of privacy which

the government may not force him to surrender to his detriment. "*In re Grand Jury Proceedings*, 632 F.2d 1033,1043 (3d Cir. 1980). Granting this order would be an irreparable and irreversible violation of Mr. Burns's rights.

III. THE FOREGONE CONCLUSION DOCTRINE DOES NOT SUPERSEDE THE FIFTH AMENDMENT AND THE CONTENTS OF MR. BURNS' DEVICES ARE NOT A FOREGONE CONCLUSION

The government concedes that forcing Mr. Burns to decrypt his devices would be testimonial but argues that the contents are a foregone conclusion and are therefore exempted from the Fifth Amendment protections. However, the evidence the government is using in part to demonstrate that foregone conclusion is information they already have access to via HD-1. In part, the government is relying on the presence of child pornography on HD-1. The government possesses Mr. Burns' HD-1 in an unlocked state. *Gov't Mot. To Decrypt*, p.18, In. 9-10.

What they are seeking is access to an entirely different hard drive, the contents of which are completely unknown to them. The government claims that Mr. Burns unequivocally stated that there was child pornography on the 2TB Hitachi Hard Drive but never establishes when or how. Mr. Burns is directly cited multiple times throughout the government's Application, but never directly in relation to child pornography on the 2TB Hitachi Hard Drive. Mr. Burns does state that the hard drive is not encrypted and that "files" are downloaded to the 2TB Hitachi

Hard Drive. Furthermore, Mr. Burns told investigators that they had seen the files he had been downloading, and thus, they should have the same files. This was said after files were found on HD-1.

When, as here, an act of production implies testimonial facts (such as possession and control), the government can *only* compel a suspect to surrender the information *if* those facts are a "foregone conclusion" already known to the government. *See Hubbell*, 530 U.S. at 44. The foregone conclusion analysis depends upon whether, prior to the compelled production, the government could have described the pertinent facts "with reasonable particularity" *Id.* at 30; *see also United States v. Ponds*, 454 F.3d 313, 320 (D.C. Cir. 2006) (holding government must prove prior knowledge of pertinent facts with "reasonable particularity" to establish "forgone conclusion").

A foregone conclusion exists only when the resulting production "adds little or nothing to the sum total of the government's information." *Fisher*, 425 U.S. at 411. For example, the government could not meet this burden in *Hubbell*, 530 U.S. at 44-45, because it had "no prior knowledge of either the existence or whereabouts" (and this did not have sufficient evidence of possession) of the thousands of pages produced by the suspect in response to a subpoena. On the other hand, in *Fisher*, a foregone conclusion was found because the government

knew that the subpoenaed documents were in the defendants' attorneys' possession and the government could independently confirm their existence and authenticity though the accountants who created them. 425 U.S. at 411.

With respect to the alternative testimonial basis of compelled decryption, two Courts of Appeals have considered this issue. *United States v. Apple Macpro Computer*, 851 F.3d 238 (3d Cir. 2017); *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012). Both opinions treat compelled decryption as a testimonial act triggering Fifth Amendment protection, and thus proceed to a foregone conclusion analysis in order to determine whether the government can force disclosure, despite the testimonial nature of the anticipated production. *See Apple Macpro*, 851 F.3d 238; *In Grand Jury Subpoena Dated March 25, 2011*, 670 F.3d at 1345-47.

The Third Circuit in *Apple Macpro* presented a foregone conclusion standard that focused on "whether the government already knows the testimony that is implicit in the act of production," in that case the particular suspect knew the password to access the encrypted hard drives. *Apple Macpro*, 851 F.3d at 249 n.7. The Third Circuit also held that no plain error was committed by the District Court in finding a foregone conclusion based upon the government's established knowledge of the contents of the hard drives. It is also important to note

the highly deferential standard of review applied in *Apple Macpro*. The underlying issue was an appeal of a contempt order so the court was required to review for plain error only. More importantly, the defendant in *Apple Macpro* forfeited his Fifth Amendment argument by failing to preserve it so the Third Circuit was not able to fully address the issue making this precedent impotent in our current circumstance. *Apple Macpro*, 851 F.3d 238 (2017). Under a more strict analysis, as is necessary in this case, the result would likely be similar to *In re Grand Jury Subpoena Dated March 25, 2011.*

Unlike the defendant in *Apple Macpro*, Mr. Burns never provided investigators with any evidence that he knew the password for the encrypted device. In his first meeting, Mr. Burns stated that the hard drive was not encrypted. In the second meeting, Mr. Burns merely stated that "it would not be in his best interest" to give a password to investigators. This statement is not an admission that he knows the actual password. Furthermore, there is no evidence that investigators inquired or confirmed where Mr. Burns obtained the drives. It is unclear if they were bought used, and perhaps was encrypted by a previous user.

The Eleventh Circuit's foregone conclusion analysis in *In re Grand Jury Subpoena Dated March 25, 2011* provided additional support for the fact that the government's requested compulsion

of decryption would not be a foregone conclusion in this case. *See* 670 F.3d at 1346-47. Agents had one specific suspect. *Id*. Substantial evidence suggested he was the sole person to access the internet from three separate internet protocol ("IP") addresses, during which time he used YouTube to share explicit materials involving minors. *Id*. at 1339. The suspect was in possession of the target hard drives when he was confronted and arrested. *Id*. Nevertheless, the court found that the government did not meet its burden to demonstrate that the testimonial act of production was a foregone conclusion. *Id.* at 1346.

The Eleventh Circuit relied in part on the fact that the suspect's production and decryption of the drivers would "be tantamount to testimony" of his "possession, control, and access to the encrypted portions of the drives' and of his capability to decrypt the files." *Id.* at 1346. The court further found that the suspect's testimonial acts were not a foregone conclusion, in part because "nothing in the record illustrates that the government knows with reasonable particularity that [the suspect] is even capable of accessing the encrypted portions of the devices. " *Id*. at 1346, 1339 n.9. *Doe*, at 210, n. 9, 108 S.Ct. 2341 (citations omitted). As the Doe majority noted: It is the "extortion of information from the accused," the attempt to force him to "disclose the contents of his own mind" that implicated the Self-Incrimination Clause. *Id*. at 211,

108 S.Ct. 2341. In *Doe II*, the Court pointed out that "neither the form nor its execution communicated any factual assertions, implicit or explicit, or conveys any information to the government." *Id.* at 215, 108 S.Ct. 2341. In the present case, forcing Mr. Burns to reveal the password for the computer communicates that factual assertion to the government, and thus, is testimonial—it requires Defendant to communicate "knowledge," unlike the production of a handwriting sample or a voice exemplar. *Id.* at 217, 108 S.Ct. 2341. *U.S. v. Kirschner*, 823 F.Supp.2d 665, 668-69 (E.D. Mich. 2010).

In this case, the government is not seeking documents or objects—it is seeking testimony from the Defendant, requiring him to divulge though his mental processes his password, that will be used to incriminate him. The government has not provided Defendant with immunity pursuant to 18 U.S.C. § 6003(a).

The *Hubbell* opinion also stated, directly relevant to the present case: Compelled testimony that communicated information that may "lead to incriminating evidence" is privileged even if the information itself is not inculpatory. *Doe v. United States*, 487 U.S. 201, 208, n.6, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988). *U.S. v. Kirschner*, 823 F.Supp.2d 665, 669 (E.D. Mich. 2010) citing *Hubbell* at 2044.

Further, both *In re Boucher* and *Fricosu* are distinguishable from the present case in yet another, essential aspect. In both cases the contents of the files subject to decryption constituted the very offense for which the defendants were indicted. In *In re Boucher,* the government agent saw the file name "2yo raped during a diaper change", which was descriptive enough to suggest that it contained child pornography. *In re Boucher*, 2009 WL 424718. For *In re Boucher*, the court required the defendant to decrypt the device after he had already opened and decrypted the device for law enforcement. The defendant was subsequently arrested and law enforcement was unable to re-open the same drive the defendant has already opened and shown to them. Unlike this case, the defendant for *In re Boucher* opened and completely decrypted the entire device contents for law enforcement. The foregone conclusion doctrine was applied because they had already seen everything that computer has to offer including specific file names and were merely trying to re-open the system that auto-locked after the defendant was arrested. As with several of the cases involving this issue, immunity became an issue. The court for *In re Boucher* still ordered that "[t]he government may not make use of Boucher's act of production to authenticate the unencrypted Z drive or its contents either before the grand jury or a petit jury." *In re Boucher*, 2009 WL 424718 at 4.

Alternately, in *U.S. v. Fricosu*, the government moved for an order-requiring defendant to produce unencrypted devices after the request for the passwords to the devices was denied. *U.S. v. Fricosu*, 841 F.Supp.2d 1232 (2012). The basis of the request was a tape-recorded phone call between the defendant and her husband in custody where they discussed the target device and its contents "essentially admitting on the tape every testimonial communication that may have been implicit in the production of the unencrypted contents." *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011* at 2012 WL 182121 at 4. Based on the dispositive conversation in *Fricosu*, the government knew the "existence" and "location" of the computer's files. *Fricosu*, 841 F.Supp.2d at 1237 (2012). Mr. Burns' two exchanges do not solidify knowledge of the existence or location of the computer's files. Furthermore, the *Fricosu* court held that the Fifth Amendment did not apply in large part because the computer at issue belonged to the wife of the accused—not the actual accused. In the case at issue, it is clear that Mr. Burns was in possession of the hard drives, and is therefore, distinguishable from *Fricosu*.

Therefore the only reason the government is now seeking to compel Mr. Burns to unlock his devices is to examine the entire contents of the devices in an effort to find any kind of evidence that might help build the government's case against Mr.

Burns. In other words, the government is seeking to recruit Mr. Burns to assist it in further investigation of the charges for which he has already been indicted, which runs against the very foundation of our adversarial legal system.

In *United States v. Doss,* 563 F.2d 265 (6th Cir.1977) (en banc), the Sixth Circuit Court of Appeals held that it was an abuse of process to call an indicted defendant before a grand jury to question him about a crime for which he has been already indicted. The Sixth Circuit did, however, hold that a previously indicted defendant can be called before a grand jury to give evidence "upon a wholly different and separable offense." *Id.* at 277.

The court specified that the subpoenaed indictee is not to be "questioned about the offense for which he stands indicted." *Id.* at 266.

The Sixth Circuit emphasized in *Doss:* When a person under our system of law has been indicted for a crime, the government has no more right to call him before a grand jury and question him about that crime than it has to call an unwilling defendant to the stand during the trial of its case. *Id.,* at 266 as cited in *United States v. Kirschner,* Supra, 823 F.Supp2d 665. Forcing Mr. Burns to decrypt his devices is the functional equivalent of calling him to testify at trial by making him concede an element of the charged offense: possession.

IV. CONCLUSION

The All Writs Act requires the writ be "necessary and appropriate" before the court can order relief. The government has only given vague details about attempts to decrypt and have made no attempt for third party intervention from the software manufacturer. They are attempting to use the "foregone conclusion" doctrine to circumvent the Fifth Amendment and take the path of least resistance by forcing Mr. Burns to be a witness against himself. The information they seek would be compelled, incriminating and testimonial and therefore implicates the protections of the Fifth Amendment. The evidence argued to create a foregone conclusion is vague at best. They have access to HD-1 and want to implicate the foregone conclusion doctrine because Mr. Burns possessed the 2TB Hitachi Hard Drive and admitted to possessing child pornography. Investigators found child pornography on HD-1. The government seeks complete entry into all digital aspects of Mr. Burn's life despite already having access to information they say they need—information they have already used to secure an indictment against Mr. Burns.

The protections offered under the Constitution are there for the protection of all and should not be so easily sidestepped. The government is required to prove their case without Mr. Burn’s assistance, and he is affirming his right to

remain silent and right not to be forced into becoming a witness against himself.

Respectfully submitted this the 15th day of March, 2019.

/s/ Dylan W. Greenwood
Attorney for Defendant
NCSB #46066
119 Brookstown Ave., Suite 300
Winston-Salem, NC 27101
(336) 661-8788
Email: Dylan@dwg-law.com

IN THE UNITED STATES DISTRICT COURT

FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

In the Matter of the Search of:		
A 2TB Hitachi Hard Drive Serial Number YFGNBBTA and Labeled HD-2	:	Case No. 1:18mj307

CERTIFICATE OF SERVICE

I, Dylan W. Greenwood, do hereby certify that on this date I served a copy of the foregoing DEFENDANT'S RESPONSE TO GOVERNMENT'S APPLICATION FOR AN ORDER TO REQUIRE DEFENDANT BURNS TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT PURSUANT TO THE ALL WRITS ACT on the United States of America by using the CM/ECF filing system, which will send notification of such filing to Eric Iverson, Assistant United States Attorney, at Eric.Iverson@usdoj.gov.

This the 15th day of March, 2019.

/s/ Dylan W. Greenwood
Attorney for Defendant
NCSB #46066
119 Brookstown Ave., Suite 300
Winston-Salem, NC 27101
(336) 661-8788
Email: Dylan@dwg-law.com